Doc Code: AP.PRE.REQ

PTO/SB/33 (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PRE-APPEAL BRIEF REQUEST FOR REVIEW	Docket Number (Optional) M4065.0486/P486	
	Application Number 09/993,495-Conf. #8165	Filed November 27, 2001
	First Named Inventor Doug Rollins	
	Art Unit 2137	Examiner S. Gelagay

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.

This request is being filed with a notice of appeal.

The review is requested for the reason(s) stated on the attached sheet(s).
Note: No more than five (5) pages may be provided.

I am the

- [ ] applicant /inventor.
- [ ] assignee of record of the entire interest. See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96)
- [x] attorney or agent of record. Registration number 28,371
- [ ] attorney or agent acting under 37 CFR 1.34. Registration number if acting under 37 CFR 1.34. _____

41,198
Signature

Thomas J. D'Amico
Typed or printed name

(202) 420-2232
Telephone number

December 11, 2009
Date

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

- [ ] *Total of 1 forms are submitted.

Docket No.: M4065.0486/P486
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Doug Rollins

Application No.: 09/993,495 | Confirmation No.: 8165

Filed: November 27, 2001 | Art Unit: 2437

For: METHOD AND APPARATUS FOR WEP KEY MANAGEMENT AND PROPAGATION IN A WIRELESS SYSTEM | Examiner: S. Gelagay

PRE-APPEAL BRIEF REQUEST FOR REVIEW

MS AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Applicant respectfully requests a review of the legal and factual bases for the rejections in the above-identified patent application. Pursuant to the guidelines set forth in the Official Gazette Notice of July 12, 2005 for the Pre-Appeal Brief Conference Program, favorable reconsideration of the subject application is respectfully requested in view of the following remarks.

Claims 1, 6-8, 14-20 and 26 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent 7,024,553 to Morimoto in view of U.S. Patent 6,055,314 to Spies, et al. ("Spies"). This rejection is respectfully traversed.

Claim 1 is directed to a method of updating and using an encryption key used by a wireless station for encrypted communications with a wired portion of the network, and recites "physically separating from said wireless station a network communications device; physically connecting said separated network communications device to an encryption key updating device

which is connected to a wired portion of said network, said wired portion of said network containing an encryption key generator for providing a new encryption key to said updating device; replacing an existing encryption key in said network communications device with a new encryption key from said generator sent over said wired portion of said network; physically reconnecting said network communications device containing said new encryption key with said wireless station of said network; and accessing said new encryption key on said network communications device during an encrypted communication."

As the Office admits, Morimoto does not teach or suggest at least "physically separating from said wireless station [the] network communications device; [and] physically connecting [the] separated network communications device to an encryption key updating device which is connected to a wired portion of said network, said wired portion of said network containing an encryption key generator for providing a new encryption key to said updating device." (Office Action, pg. 3).

Applicant submits that the Office's characterizations of the teachings of ¶¶ [0021-0026] of the specification are incorrect and, contrary to what the Office suggests, are *not* consistent with the teachings of Morimoto. Although the present application and Morimoto are both directed to updating encryption keys on a corporate network, their methods are quite different. Morimoto explicitly teaches that "each of STAs 103 memorizes and supervises ... [new] encrypted key[s] delivered from the key management server 101 [wirelessly] through the AP 102 and has communication with the AP using the encrypted key[s]." (Morimoto, col. 7, lns. 62—col. 8, ln. 5, emphasis added). By contrast, the present application teaches updating the encryption key in use *on the access point itself*, and also updating the encryption key on the updating device (*e.g.*, a PC card tray 400), so that wireless communications devices can be *physically* connected to that device for updating. (¶ [0027]-[0028]). This is especially important because the present application contemplates and distinguishes itself from a system such as described in Morimoto, discussing in ¶ [0008] that "[i]f the vendor supplies a management application that supports automatic propagation to access points, that may be used... [but i]f the vendor supplied management application does not... then..." the process described in the present application could be used. (¶ [0008]).

Returning to Morimoto and considering the discussion above, Morimoto in fact explicitly teaches away from the claimed concept of physical attachment of a separated network communications device to a wired encryption key updating device (which is not an access point) for encryption key distribution, as recited by claim 1. When a reference teaches away, "[i]t is improper to combine." MPEP § 2145(X)(D)(2). Accordingly, even if Spies taught "physically separating from said wireless station [the] network communications device; [and] physically connecting [the] separated network communications device to an encryption key updating device," which as explained below, it does not, combination of the references would be improper. Moreover, combination of Morimoto with the teachings of Spies would frustrate the very purpose of Morimoto's teachings (updating encryption keys *wirelessly*), and "the claimed combination cannot change the principle of operation of the primary reference or render the reference inoperable for its intended purpose." MPEP § 2143.01.

Applicant submits that Spies, which is directed to a method for secure purchase and delivery of video programs, cannot cure the deficiencies of Morimoto even if the references could be combined. Spies merely teaches distributing decryption keys on removable IC cards (e.g., PCMCIA cards) to enable a video player to decode *video content* stored on a DVD or other medium—Spies' IC cards are not network communications devices, nor do they provide "encryption key[s] used by a wireless station for encrypted communications with a wired portion of the network." (Spies, Abstract, col. 6, lns. 19-33). In fact, Spies does not teach or suggest network encryption, much less "physically separating from said wireless station [a] network communications device; [and] physically connecting [the] separated network communications device to an encryption key updating device," as recited in claim 1. Spies' teachings would not permit "accessing said new encryption key on said network communications device during an encrypted communication," as claimed, because Spies only teaches use of a *decryption* key to decode *specific* encrypted video content. Moreover, the IC card of Spies is not a "separated network communications device."

For all these reasons, claim 1 is believed to be allowable over the Morimoto and Spies combination.

Claims 6-7 depend from claim 1 and are believed to be allowable for at least the same reasons, as well as on their own merit.

Claim 8 recites similar limitations to claim 1, namely "a wireless network communications device containing [an] encryption key, said wireless station configured to access said encryption key on said wireless network communications device during said encrypted communications, said wireless network communications device being physically disconnectable from said wireless station and physically connectable to [a] wired encryption key updating device wired to said network to receive, store, and use a new encryption key which is configured to be transmitted over said wired network by said wired network communications device," and is believed to be allowable over the Morimoto and Spies combination for at least the same reasons as claim 1, as well as on its own merit. Claim 14 depends from claim 8 and is believed to be allowable for at least the same reasons, as well as on its own merit.

Claims 15, 17 and 20 also recite similar limitations to claim 1, namely "said wireless network communications device being physically removable from said station and storing an updateable encryption key used in conducting encrypted wireless communications from said wireless network station, said removable wireless network communications device being physically connectable to a wired network to receive, store, and use a new encryption key, said wireless station configured to access an encryption key on said wireless network communications device during a wireless communication," (Claim 15), "a storage area on said network card which stores an updateable encryption key for use by a wireless station when conducting encrypted wireless network communications, said encryption key being updateable when said card is physically connected to a wired network card interface which supplies a new encryption key, said wireless station configured to access said new encryption key on said wireless network communications device during a wireless communication," (Claim 17), and "a programming device connected to said wired network for receiving over a wire connection a new encryption key from said generator, said programming device being adapted to physically receive a wireless network communications device containing an updatable encryption key and storing said received encryption key in said wireless network communications device, said new encryption key on said wireless network

communications device being accessible by a wireless network device during encrypted communications," (Claim 20), and are believed to be allowable over the Morimoto and Spies combination for at least the same reasons as claim 1, as well as on their own merit. Claims 16, 18-19 and 26 depend from claims 15, 17, and 20 respectively, and are likewise allowable. Accordingly, Applicant respectfully requests that the rejection be withdrawn and the claims allowed.

Claims 2-3, 9-10, and 21-23 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Morimoto in view of Spies and in further view of U.S. Pat. No. 4,369,332 to Campbell, Jr. ("Campbell"). This rejection is respectfully traversed.

Claims 2-3, 9-10 and 21-23 depend from claims 1, 8 and 20, and are allowable over the Morimoto and Spies combination for at least the same reasons discussed above with respect to claims 1, 8 and 20. Campbell, which is cited by the Office as teaching encryption key regeneration at specific or user-defined intervals, cannot cure the deficiencies of the inoperable and incompatible Morimoto and Spies combination discussed above. (Office Action, pg. 8). Accordingly, Applicant respectfully requests that the rejection be withdrawn and the claims allowed.

Claims 4-5, 11-12 and 24-25 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Morimoto in view of Spies and in further view of U.S. Pat. No. 6,226,750 to Trieger ("Trieger"). This rejection is respectfully traversed.

Claims 4-5, 11-12 and 24-25 depend from claims 1, 8 and 20, and are allowable over the Morimoto and Spies combination for at least the same reasons discussed above with respect to claims 1, 8 and 20. Trieger, which is cited by the Office as teaching comparison of newly-generated encryption keys to previous keys to ensure there is no repetition, cannot cure the deficiencies of Morimoto and Spies discussed above. (Office Action, pg. 8). Accordingly, Applicant respectfully requests that the rejection be withdrawn and the claims allowed.

Applicant respectfully submits that the pending claims are patentable over the cited art. Applicant reserves the right to pursue additional arguments on appeal, especially with respect to the dependent claims. Favorable consideration and a Notice of Allowance are solicited.